1865 THE UNIVERSITY OF MAINE

Join us for this free webinar series!

Register online:
ai.umaine.edu

Moderated by Ali Abedi,
Associate Vice President for Research
University of Maine

Sponsored by IEEE
Maine COM/CS Chapter

IEEE
Advancing Technology for Humanity

UMaine Artificial Intelligence

AI for Secure IoT Design

Thursday, February 2, 2023
12:00 - 1:00 p.m. EST (live via Zoom)

Prabuddha Chakraborty
Assistant Professor, Electrical & Computer Engineering
Advanced Structures & Composites Center
University of Maine

Prabuddha Chakraborty's research interest lies in the intersecting areas of Artificial Intelligence, Internet-of-Things, and system security. He received his PhD in Electrical and Computer Engineering from the University of Florida. He has worked within the Security Software Team at Texas Instruments and the FPGA acceleration R&D team at Xilinx. His research effort has so far led to more than 20 peer-reviewed journal/conference articles and more than 10 US patents & copyrights (filed/granted). He is a recipient of the Certificate of Outstanding Merit (University of Florida in 2021), for his academic and research excellence. He has also received several awards/honors for his research contributions including the TTTC's E. J. McCluskey Best Doctoral Thesis Award 2022, Best Hardware Demo Award (at IEEE HOST 2019) and the Top Picks in Hardware and Embedded Security award 2021 (by IEEE HSTTC).

Leveraging Artificial Intelligence Towards Establishing a Robust Hardware Root-of-Trust for Edge Devices

Intelligent edge devices have become prevalent in the emergent Internet of Things (IoT) era for a multitude of sensing and automation tasks that help improve our lives and transform our industry. These systems are being increasingly deployed in diverse domains, such as smart transportation, precision agriculture, space explorations, satellite sensing, smart healthcare, and industrial automation. They are often designed to meet tight resource constraints in power, performance, cost, and communication bandwidth while addressing many critical security threats. In this talk we will discuss several artificial intelligence (AI)-guided techniques to improve the security of electronic hardware against various attacks, considering the untrusted supply chain, to establish a robust hardware root of trust for edge devices. Specifically, we will discuss (i) an approach for creating low-overhead attack-resistant hardware that can protect itself from reverse engineering, piracy, and malicious modifications, and (ii) a unified AI-guided framework for detecting malicious hardware design modifications at different stages of the electronic device lifecycle.

In complying with the letter and spirit of applicable laws and pursuing its own goals of diversity, the University of Maine System does not discriminate on the grounds of race, color, religion, sex, sexual orientation, transgender status, gender, gender identity or expression, ethnicity, national origin, citizenship status, familial status, ancestry, age, disability physical or mental, genetic information, or veterans or military status in employment, education, and all other programs and activities. The University provides reasonable accommodations to qualified individuals with disabilities upon request. The following person has been designated to handle inquiries regarding non-discrimination policies: Director of Equal Opportunity, 101 Boudreau Hall, University of Maine, Orono, ME 04469-5754, 207.581.1226, TTY 711 (Maine Relay System).